СЕКЦИЯ 4.
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

УДК 004.492.2

А. А. Амирова, Е. Ю. Кузин
Научный руководитель: канд. ф.-м. наук, доц. Н. И. Черкасова
Московский государственный тенический университет
гражданской авиации, Москва

ОСОБЕННОСТИ ПРОБЛЕМ БЕЗОПАСНОСТИ ВТОРОГО УРОВНЯ АРХИТЕКТУРЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ

Аннотация. Безопасность любой информационно-аналитической системы является важнейшим фактором, поэтому исследование рисков, возникающих на втором уровне архитектуры аналитических систем, а именно их процессов и инструментов, является одной из актуальных тем исследования и поддержания высокой функциональности и работоспособности всех информационно-аналитических систем обеспечения безопасности. В работе рассмотрены основные проблемы, требующие разрешения при реализации информационно-аналитических систем безопасности с учетом основных функций ETL-систем и процессов второго уровня архитектуры.

Ключевые слова: процесс; валидация; архитектура аналитических систем; безопасность; ETL-системы.

Важнейшим фактором любой информационно-аналитической системы является безопасность на всех шести уровнях архитектуры: накопление и исход-

ная обработка; получение, конвертация и загрузка; складирование и распределение; преобразование в витринный тип; анализ и исследование; web-источник.

В работе представлены исследования рисков, возникающих на втором уровне информационно-аналитических систем, а именно процессов получения, конвертации и загрузки информации.

Информационно-аналитические системы безопасности — это прежде всего системы, позволяющие получать, обрабатывать и проводить различные операции над информацией, иными словами — анализировать ее [1]. Отметим при этом, что качество обработки и оценка получаемых данных — это качество и успех деятельности при работе с информационным материалом.

Рассмотрим особенности ETL-инструментов второго уровня информационно-аналитической системы, процессов, которые совершают извлечение (extraction), преобразование (transformation) и загрузку данных (loading) [2]. Функциональные особенности этих процессов представляются следующим образом:

1. Предназначение процесса извлечения помогает совершить получение данных из источников, находящихся на нижних уровнях.

2. В ходе работы преобразования информации происходит ликвидация избытка данных. Это реализуется за счет проведения вычислений и агрегаций.

3. Извлечение, загрузка и преобразование могут быть трехступенчатыми, но их использование зарезервированного регламента.

На рис. 1 представлены все основные функции ETL-систем.

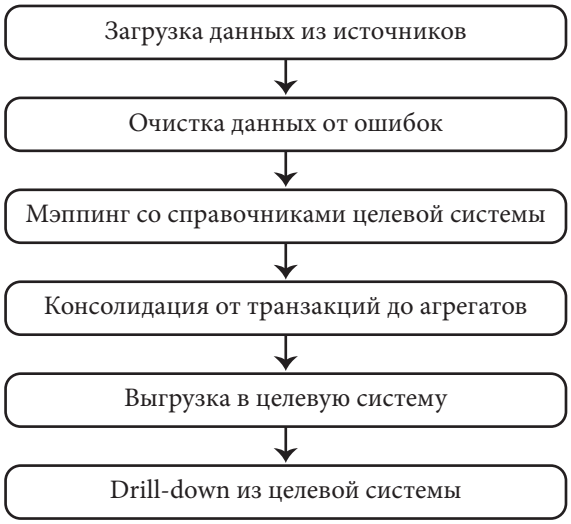

Рис. 1. Основные функции второго уровня
архитектуры информационно-аналитических систем

Проблема, из-за которой в принципе родилась необходимость использовать решения ETL, заключается в потребностях бизнеса в получении достоверной отчетности из данных любой ERP-системы.

Для выявления проблем и рисков, требующих разрешения при работе с информационно-аналитической системой, рассмотрим каждый процесс ETL-инструментов в отдельности.

1. Процесс загрузки. Задача данного процесса — представить в ETL данные произвольного качества для дальнейшей обработки, но отметим, что на этом этапе важно сверить суммы пришедших строк, так как если в исходной системе больше строк, чем в RawData, то это означает, что загрузка прошла с ошибкой.

2. Процесс валидации данных. Данный процесс является важным, поскольку на этом этапе данные последовательно проверяются на корректность и полноту, и составляется отчет об ошибках для исправления.

3. Процесс мэппинга (графическое представление процедуры, процесса, структуры или системы, отражающее расположение или отношения компонентов и документирующее информационные потоки). Реализация данного процесса осуществляется по следующему алгоритму: к валидированной таблице пристраивается еще *n*-столбцов по количеству справочников целевой модели данных, а потом по таблицам мэппингов в каждой пристроенной ячейке, в каждой строке проставляются значения целевых справочников. Значения могут проставляться как 1:1, так и *:1, так и 1:* и *:*, для настройки последних двух вариантов используют формулы и скрипты мэппинга, реализованные в ETL-инструменте.

4. Процесс агрегации данных. Из-за разности детализации данных в OLTP-системах (Online Transaction Processing) и OLAP-системах (Online Analytical Processing, аналитическая обработка в реальном времени) данный процесс является очень важным. OLAP-системы — это полностью денормализованная таблица фактов и окружающие ее таблицы справочников (звездочка/снежинка, см. процесс мэппинга), при том что максимальная детализация сумм OLAP — это количество перестановок всех элементов всех справочников. А OLTP система может содержать несколько сумм для одного и того же набора элементов справочников [3].

5. Выгрузка в целевую систему — это технический процесс использования коннектора и передачи данных в целевую систему.

В заключение можно отметить, что в условиях все более возрастающей интеграции информационных технологий в современный мир, а также растущей вероятности появления рисков и вторжений в информационное пространство следует строить информационно-аналитическое обеспечение безопасности с учетом общемирового опыта. В этой связи крайне необходимо, чтобы применяемые в таких системах информационные технологии соответствовали

международным стандартам интерфейса с различными базами данных визуализации связей и обмена аналитической информацией.

Список литературы

1. URL: http://www.e-biblio.ru/book/bib/01_informatika/IAS/Book.html
2. URL: http://itdirector.org.ua/club/My_forum/forum10/topic19/
3. URL: http://life-prog.ru/1_759_OLTP — i-OLAP-tehnologii.html

УДК 654.072.7

С. С. Блинов
Научный руководитель: ст. преп. В. В. Шкитенков
Уральский федеральный университет, Екатеринбург

ИДЕНТИФИКАЦИЯ БАЗОВЫХ СТАНЦИЙ ОПЕРАТОРОВ СОТОВОЙ СВЯЗИ С ПОМОЩЬЮ ПОРТАТИВНОГО КОМПЛЕКСА РАДИОКОНТРОЛЯ

Аннотация. В статье рассматривается проблема незаконного использования радиочастотного ресурса и алгоритмы идентификации базовых станций, эксплуатируемых операторами сотовой связи с нарушением законодательства Российской Федерации.

Ключевые слова: базовая станция; GSM; UMTS; LTE аппаратно-программный комплекс; радиоэлектронная обстановка; радиоконтроль; сотовая связь.

На 2017 год Роскомнадзором было выявлено более 13000 базовых станций, установленных с нарушением законов РФ [1] или не имеющих разрешения на использование частот. Для выявления таких базовых станций Радиочастноным центром проводятся периодические мероприятия радиоконтроля. Для анализа и контроля радиоэлектронной обстановки используются мобильные комплексы радиоконтроля. Всех их объединяют большие габариты и огромная стоимость — более 10 млн рублей за одно устройство. Это обусловлено тем, что для использования таких комплексов требуется переоборудование дорогих автомобилей, таких как Ford Transit или Toyota Land Cruiser, а для питания комплексов требуются мощные дизель-генераторы [2].

Следовательно, можно сформулировать цель — разработка портативного устройства для измерение радиоэлектронной обстановки в сетях сотовой связи стандартов GSM, UMTS и LTE, которое будет значительно дешевле и компактнее ныне существующих.